REMARKS/ARGUMENTS

These remarks are in response to the Final Office Action dated July 19, 2004. Claims 1-13 are pending and finally rejected.

The Examiner rejected claims 1-13 under 35 U.S.C. § 103(a) as being unpatentable over Musgrave et al. (U.S. Patent No. 6,202,151) in view of Gilchrist (U.S. Patent No. 6,167,517). In so doing, the Examiner stated:

> In regards to claim 1, 6-8, and 13, Musgrave discloses a biometric certificate which may be generated by concatenating transaction data, a public key, and the set of data, including the biometric data (Musgrave: column 4, lines 53-55). This meets the limitation of "capturing biometric information of a user; encrypting using server public key." The authenticating certificate is then hashed to generate a hashed value. The hashed value is then sent to a registration authority having a biometric certificate generated where the hashed value is then signed; that is, encrypted, using the private key of the user to generate a digital signature incorporating the biometric data. The digital signature is then appended to the transaction data (Musgrave: Column 5, lines 15-35). This meets the limitation of "signing the biometric information with a client private key." After receiving the electronic transaction from the network a receiver decrypts the transaction using it's private key, de-hashes the decrypted transaction and extracts the biometric certificate. The receiver then sends the biometric certificate to the biometric certificate management system (BCMS) for authentication (Musgrave: column 5, lines 36-47). This meets the limitation of "sending the encrypted and signed data to a secure server in the network; accepting and verifying credentials associated with the signed and encrypted data from the server utilizing the public key from the central server."
>
> Musgrave discloses that "since private keys are physically stored on computers and/or electronic storage devices, such private keys are not physically related to the entities associated with the private keys. For example, a private (Musgrave: column 2, lines 40-45).." Since the private key is stored on computers and are physically realted [sic] to the devices on which they are stored on it would be possible to tell fro which device a signature using a private key came. Musgrave discloses that "private keys are not limited to actual human indifviuals [sic] (Musgrave: column 2, line 46)." This is interpreted as meanting [sic] the private keys can be associated with devices on which they are stored. This meets the limitation of "private key of the computer system." Musgrave also discloses that "after receiving the electronic transaction from the network, a receiver decrypts the electronic tranaction [sic] using its private key" (Musgrave: column 5, lines 36-38). This meets the limitation of "encrypting the biometric information using a secure server's public key" since in asymmetric cryptography

> if you decrypt a message with a private key the message must have been encrypted with a the corresponding public key.
>
> However, Musgrave does not disclose "installing the credentials into the computer if the credentials are verified."
>
> Gilchrist discloses the biometric template is stored locally on the client system and discloses adding new templates to the system (Gilchrist: column 1, lines 51-65). This meets the limitation of "installing the credentials into the computer if the credentials are verified."
>
> It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of authentication using a biometric authenticating certificate as disclosed by Musgrave with the method of storing the biometric template locally as disclosed by Gilchrist in order to guard against a malicious user who substitutes another template to gain unauthorized access to the host system (Gilchrist: abstract).

Applicants respectfully disagree.

In a method and system of the present invention, a user can walk up to any client computer system within an enterprise and have his/her individual credentials, e.g., PKI certificate and keys, securely imported to and installed onto the client computer system after the user has been authenticated by a central server. In the preferred embodiment, biometric information from the user is used to authenticate the user such that authentication is performed without a memory token. Once installed, the user's credentials are utilized to authorize the user for subsequent use of the client computer system during a session. When the session is terminated, the user's credentials are permanently removed from the client computer system.

The present invention, as recited in claims 1 and 7, provides:

> 1. A method for providing an authentication of a user of a computer in a network, the method comprising the steps of:
>
> (a) capturing biometric information of the user by the computer;
>
> (b) encrypting the biometric information using a secure server's public key and signing the biometric information with a private key of the computer system;
>
> (c) sending the encrypted and signed information from the computer to the secure server in the network;
>
> (d) accepting and verifying credentials associated with the signed and encrypted information from the secure server utilizing the public key from the secure server; and

(e) installing the credentials into the computer if the credentials are verified.

7. (Currently amended) A system for providing an authentication of a user of a computer system in a network; the system comprising:

a secure server coupled to the computer system for authenticating biometric information of the user, wherein the secure server includes a database that stores credential information associated with biometric information; and

a biometric capture device within the computer system for receiving the biometric information of the user and sending the biometric information to the secure server,

wherein if the secure server authenticates the user via the biometric information, the secure server sends the associated credential information to the computer system such that the user can securely operate the computer system.

In contrast to the present invention, Musgrave is directed to a method for combining biometric identification with a digital certificate for electronic authentication of a user. (Abstract). In Musgrave, a biometric certificate incorporates the user's biometric data with the user's credentials such that the certificate physically verifies the identity of the user. The biometric certificate is appended to transaction data to form an electronic transaction, which is then transmitted to and received by a central server for authentication. If the user is authenticated, the transaction is processed. (Column 5, line 27-column 6, line 18).

Gilchrist is directed to authenticating a user via the user's biometric data. In Gilchrist, biometric templates are stored at a centralized repository accessible by one or more servers. Client computer systems are coupled to the servers. When the user wishes to access resources on a server via a client computer system, the biometric template associated with the user is compared to a biometric sample provided by the user to authenticate the user. (Column 4, lines 25-38).

Together, Musgrave and Gilchrist teach authenticating a user by comparing a sample of the user's biometric information with a template stored in a central repository of templates. The biometric sample is disguised by a collecting computer system and transmitted to an authentication server for comparison.

Applicants respectfully submit that neither reference, alone or in combination, teaches or suggests the cooperation of elements as recited in claims 1 and 7. With regard to claim 1, neither reference teaches or suggests, "encrypting the biometric information using a secure server's public key and signing the biometric information with a private key of the computer system" in the network, as recited in claim 1. In the present invention, the computer that the user wishes to use is equipped to capture a sample of the user's biometric information. Before sending the sample to the central server for authentication, the computer performs *two* security steps: (1) it *encrypts* the sample using the central server's public key; and (2) it *signs* the sample with its private key. It is notable that the sample *is not* and *cannot be* signed by the user because the user's credentials are not resident on the computer.

In Musgrave, an authenticating certificate, which includes a sample of biometric data collected from the user, is *hashed* to generate a hashed value. Before transmitting the sample to a receiver for authentication, the hashed value is then signed "using *the private key of the user* to generate a digital signature, incorporating the biometric data." (Column 5, lines 15-32). In Gilchrist, the computer computes a message digest from the sample and other data, and transmits the message digest to the host for authentication. (Column 6, lines 22-29). Nothing in Musgrave or Gilchrist teaches or suggests encrypting the sample using the server's *public key* AND signing the sample with the *computer's*, as opposed to the user's, private key, as recited in claim 1.

In the Office Action, the Examiner contends that the *user's* private key *is* the *computer's* private key because private keys in general are stored on computers and are purportedly associated with the computer on which they are stored. Applicants respectfully disagree. In public key cryptography, the key pair (private/public key) is unique to one entity, e.g., a user, an organization, a computer, or a server. Consequently, a user using a computer system cannot use his/her private key to decrypt a message encrypted by the computer system's public key, just as the computer system cannot user its public key to decrypt a message encrypted by the user's private key. The fact that both keys might be stored on the computer system is immaterial. Accordingly, Applicants respectfully submit that the user's private key in Musgrave cannot be construed to be the computer system's private key in the present invention.

In addition, Applicants respectfully submit that Musgrave in view of Gilchrist fails to teach or suggest "accepting and verifying credentials . . . *from* the secure server utilizing the *public key* from the secure server," as recited in claim 1. In the present invention, after the server authenticates the user by decrypting the sample and positively comparing the sample to a biometric template, the server retrieves credentials associated with the user, signs the credentials with the server's private key, and sends the signed credentials back to the computer. The computer utilizes the server's public key to verify that the credentials came from the server.

In Musgrave, the receiver decrypts the biometric certificate utilizing its *private key* (column 5, lines 36-39) and sends the biometric certificate to a biometric certificate management system (BCMS) for authentication. The BCMS generates an authentication decision indicating verification of the authenticity of the user. (Column 5, line 44 to column 6, line 11). In Gilchrist, the biometric authentication service manages biometric templates and authentication policies. Credentials are verified by comparing message digests. Applicants respectfully submit that neither Musgrave nor Gilchrist teach or suggest "accepting and verifying credentials . . . from the secure server utilizing the *public key* from the secure server," as recited in claim 1.

Finally, with regard to claim 1, Applicants respectfully submit that neither reference teaches or suggests "installing the credentials into the computer *if the credentials are verified.*" In the Office Action, the Examiner concedes that Musgrave fails to teach this element, but contends that Gilchrist teaches storing biometric templates locally on a client system at column 1, lines 51-65. Applicants respectfully disagree.

In the present invention, a user's credentials allow the user to perform secure transactions with another party, such as a server. Credentials include PKI certificates and keys. When the user utilizes his/her/its credentials, both parties in the secure transaction are assured that the transaction is *secure*, i.e., the information passed between the parties will not be compromised or discovered by an intruder.

Gilchrist is directed only to authenticating the user through his/her biometric information. While biometric information positively identifies the user, it cannot be used to provide *secure* transactions. Applicants respectfully submit that credentials *do not* include biometric information, and that Gilchrist makes no mention of credentials or installing credentials on a computer system utilized by the user.

Even if biometric information were to be construed to be a credential, which it is not, Gilchrist still does not teach or suggest installing the user's biometric information on the computer system *if the biometric information is verified.* In Gilchrist, if the biometric sample matches the template, the user is simply granted access to the host system. (Column 4, lines 36-38). Nothing is said or suggested about "installing" the user's biometric information locally on the computer. The cited portion of Gilchrist merely states that biometric templates are stored locally on a client system, but does not mention that they are install therein if the samples are verified. Indeed, storing templates locally would significantly compromise both Musgrave and Gilchrist because then an intruder could break into the client computer to steal an authorized user's template and submit the stolen template as the live sample in order to break into the host.

Based on the reasons above, Applicants respectfully submit that Musgrave in view of Gilchrist fails to teach or suggest the present invention, as recited in claim 1. Accordingly, claim

1 is allowable over the cited references. Because claims 2-6 depend on claim 1, Applicants respectfully submit that claims 2-6 are also allowable over the cited references.

With regard to claim 7, Applicants respectfully submit that neither Musgrave nor Gilchrist teach or suggest a secure server that "stores credential information associated with biometric information." In addition, neither reference teaches or suggests a secure server that "sends the associated credential information to the computer system" if the secure server authenticates the user "such that the user can securely operate the computer system."

As stated above, neither Musgrave nor Gilchrist are concerned about "credential information associated with biometric information," because both references are directed only to authenticating a user. Accordingly, the only things stored are templates, which are not credentials. Moreover, as stated above, neither reference sends anything, let alone credentials, to the computer system "if the secure server authenticates the user via the biometric information," as recite in claim 7.

Applicants respectfully submit that claim 7 is allowable over the cited references. Because claims 8-13 depend on claim 7, Applicants respectfully submit that claims 8-13 are also allowable over the cited references.

In view of the foregoing, it is submitted that the claims 1-13 are allowable over the cited references and are in condition for allowance. Applicants respectfully request reconsideration of the rejections and objections to the claims.

Applicants' attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

September 14, 2004
Date

Joyce Tom
Attorney for Applicant(s)
Reg. No. 48,681
(650) 493-4540